REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 09-04-2009	**2. REPORT TYPE** Final Report	**3. DATES COVERED** *(From - To)* March 1, 2008 - January 31, 2009

4. TITLE AND SUBTITLE Quantum Strategies: Proposal to Experimentally Test a Quantum Economics Protocol Final Report	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** W31P4Q-08-1-0006 **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) Joseph B. Altepeter and Prem Kumar	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Northwestern University, EECS Department 2145 Sheridan Road Evanston, IL 60208-3118, USA	**8. PERFORMING ORGANIZATION REPORT NUMBER** SP0001986_Final-Report
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army Aviation and Missile Command Special Contracts and Support Division/AMSAM-AC_RD_RA Redstone Arsenal, AL 35898-5280 (Attn: Ms. Donna Smith, 256-842-8707)	**10. SPONSOR/MONITOR'S ACRONYM(S)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION/AVAILABILITY STATEMENT

Distribution unlimited. Fundamental research exempt from prepublications controls.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

In order to demonstrate the feasibility of quantum games, we proposed to implement a proof-of-principle quantum public goods game, and to experimentally demonstrate that the quantum performance of the game exceeds the ideal performance of its classical analogue. We have successfully implemented such a game, and its experimental performance clearly exceeds the ideal performance of the classical public goods game. In fact, the ratio of the quantum to classical performance increases linearly with the number of players. Measured player expectation for the quantum game was measured to be within statistical error of theoretical predictions.

15. SUBJECT TERMS

Quantum Games; Quantum Information; Quantum Communication

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(Include area code)*
U	U	U		31	

Quantum Strategies: Proposal to Experimentally Test a Quantum Economics Protocol
FINAL REPORT

April 9th, 2009

Sponsored By
Defense Advanced Research Projects Agency (DOD)
Defense Sciences Office
ARPA Order No. AM09-00

Issued By U.S. Army Aviation and Missile Research, Development, and
Engineering Center under Grant No. W31P4Q-08-1-0006

Name of Grantee:	Northwestern University
Principal Investigator:	Prem Kumar
Business Address:	EECS Department Northwestern University 2145 Sheridan Road Evanston, IL 60208-3118, USA
Phone Number:	(847) 491-4128
Effective Date of Grant:	3/1/08
Short Title of Work:	Quantum Games
Grant Expiration Date:	1/31/09
Reporting Period:	3/1/08–1/31/09

DISCLAIMER

"The views and conclusions in contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Defense Advanced Research Projects Agency; the U.S. Army Aviation and Missile Research, Development, and Engineering Center; or the U.S. Government."

Contents

1 Executive Summary

In order to demonstrate the feasibility of quantum games, we proposed to implement a proof-of-principle quantum public goods game, and to experimentally demonstrate that the quantum performance of the game exceeds the ideal performance of its classical analogue. We have successfully implemented such a game, and its experimental performance clearly exceeds the ideal performance of the classical public goods game. In fact, the ratio of the quantum to classical performance increases linearly with the number of players. Measured player expectation for the quantum game was measured to be within statistical error of theoretical predictions.

In order to experimentally implement the quantum public goods game, several key experimental and theoretical developments were necessary. The key experimental components were a frequency-degenerate source of entangled photon pairs, a two-qubit entangling gate (such as a controlled-NOT gate), and four fast single-photon detectors acting as a measurement array. The entangled photon source is the first telecom-band source of degenerate-frequency entangled photons, and was characterized to have a 96 ± 1% fidelity with a maximally entangled state and a 97 ± 4% Hong-Ou-Mandel dip visibility. This source utilizes reverse Hong-Ou-Mandel interference inside a Sagnac-loop configuration to deterministically split identical photon pairs into separate spatial modes. The quantum controlled-NOT gate performs the entangling operation which links player actions. Its process fidelity was bounded to be between 91% and 95%. As part of the CNOT measurement process, we additionally developed a new method of detecting and compensating for systematic errors in multi-qubit quantum processes.

Theoretical progress began with the formalization of the quantum public goods game and the classification of its equilibria. This classification was successfully performed for all proposed versions of the quantum game. The most significant theoretical insight gained during this work, however, concerns the reclassification of quantum games as adversarial quantum communications protocols (in contrast to cooperative quantum communications protocols, such as quantum key distribution). From within this broader class of adversarial protocols we performed a detailed analysis of the SYMMETRIC PRIVATE INFORMATION RETRIEVAL protocol, and conclude that it is an ideal candidate for near-term experimental implementation.

This report is organized as follows. Section 2 briefly reviews the proposed work. Section 3 details the development and characterization of the first LOQC-compatible source of telecom-band entangled photon pairs. Section 4 discusses the development and characterization of the entangling quantum controlled-NOT gate. Section 5 briefly discusses the detector array. Section 6 details the implementation of the quantum game itself. Section 7 summarizes theoretical work performed as part of the seedling. Finally, Section 8 summarizes these results and provides a list of all milestones and relevant metrics.

2 Review of the Seedling Proposal

In order to demonstrate the feasibility of quantum games, we proposed to experimentally implement a proof-of-principle quantum public goods game, and to experimentally demonstrate that the quantum performance of that game exceeds the ideal performance of its classical analogue. This (now successful) implementation would demonstrate the functionality of key experimental components of optical quantum games: sources of entangled photon pairs, reliable single-qubit transformations, and high-fidelity two-qubit entangling operations. In addition, this would be the first proof-of-principle realization of a multi-party quantum game—the key first step towards the more complicated and general quantum protocols which would be the focus of a full program on quantum games.

2.1 The Classical Public Goods Game

Here we define a simple version of a more general public goods game [1]. In this game, there are only two goods of value, the public good and the private good. Each player possesses some amount of the private good, which can be thought of as their personal wealth. The public good is equally valuable to all players, and each player receives the full benefit of the public good. In other words, if the public good was \$1, then each player would value it as if they had an extra \$1 of their private good. The goal of each player is to play the game in such a way that the sum of the public good and their individual private good is maximized. The players in the game have the option of using some or all of their private good for the purpose of increasing the public good. The sole choice each player receives when playing the game is whether or not to contribute to the public good. Before analyzing the outcome of this game, we define the variables involved:

n	Number of players, indexed by k,
y_k	Initial endowment of private good for player k,
c_k	Amount of contribution of player k to the public good, and
$x(c_1, \ldots, c_k)$	Amount of public good as a function of total contributions.
E_k	Final expectation per player, equal to $x(c_1, \ldots, c_k) + y_k - c_k$.

In order to study the dynamics of the game, it is necessary to know how personal contributions increase the public good. We assume private contributions linearly increase the public good, such that:

$$x(c_1, \ldots, c_k) = \sum_k \frac{ac_k}{n} \tag{1}$$

where a/n is the rate at which private contributions (c) are transformed into the public good (x). For ease of analysis, assume that each player starts with 1 unit of private good ($y_k = 1$). Further assume that each player must choose to donate either all of their private good (contribute) or none of it (defect). For the case where $a < 1$, it is always rational and efficient for each player to defect (even if everyone contributes, no one will benefit). For $a > n$, it is always rational and efficient for each player to contribute (even if only one player contributes, that player will still benefit).

The case of interest is when:

$$1 < a < n. \tag{2}$$

Here the rational, equilibrium outcome is for every player to defect, creating an expectation per player of

$$E_k = 1. \tag{3}$$

In contrast, the efficient outcome is when every player contributes, increasing the expectation to:

$$E_k = a. \tag{4}$$

The goal of a quantum extension of this classical game is to use entanglement and quantum measurement to extend a player's choices such that a rational equilibrium exists which is more efficient that the classical maximum of $E_k = 1$.

2.2 The Quantum Public Goods Game

A quantum extension to this classical game was first proposed by Chen, Hogg, and Beausoleil [1], and is summarized here. This quantum protocol models a players choice of whether to contribute or defect as a probabilistic combination of unitary operations on shared entangled photon pairs. Unitary operations exist which model the classical choices of "contribute" or "defect", and if each player restricts themselves to only these choices, then the classical game will be exactly reproduced. However, because any general quantum operation is allowed, the players' strategies can be extended to take advantage of the entanglement shared between players. Taking into account these more general operations, it can be proven that a rational equilibrium exists which has greater expectation per player than in the classical game.

The physical operation of the protocol is shown in Figure 1, and consists of the following steps:

1. The referee distributes entangled photon pairs to the players. Each player shares one half of an entangled pair with each of their nearest neighbors.

2. Players perform quantum operations on the two photons they control and return the photons to the referee. These quantum operations implement each player's strategy.

3. The referee applies an entangling operation, equivalent to a CNOT gate and a basis transformation, to each of the photon pairs.

4. A measurement is made on each photon. If either of a player's photons is measured in the "0" state, that player is required to contribute. If both of a player's photons are measured in the "1" state, that player defects (does not contribute). (An alternate implementation of the game allows partial contributions; in this version a player's contribution is proportional to the number of measured "0" states among their photons.)

While the protocol described above distributes entanglement only to nearest neighbors, this protocol could also be carried out by distributing entangled pairs between each player and each other player (full pair-wise entanglement). The latter variation requires more entangled states and more quantum gates, but results in a higher expectation per player.

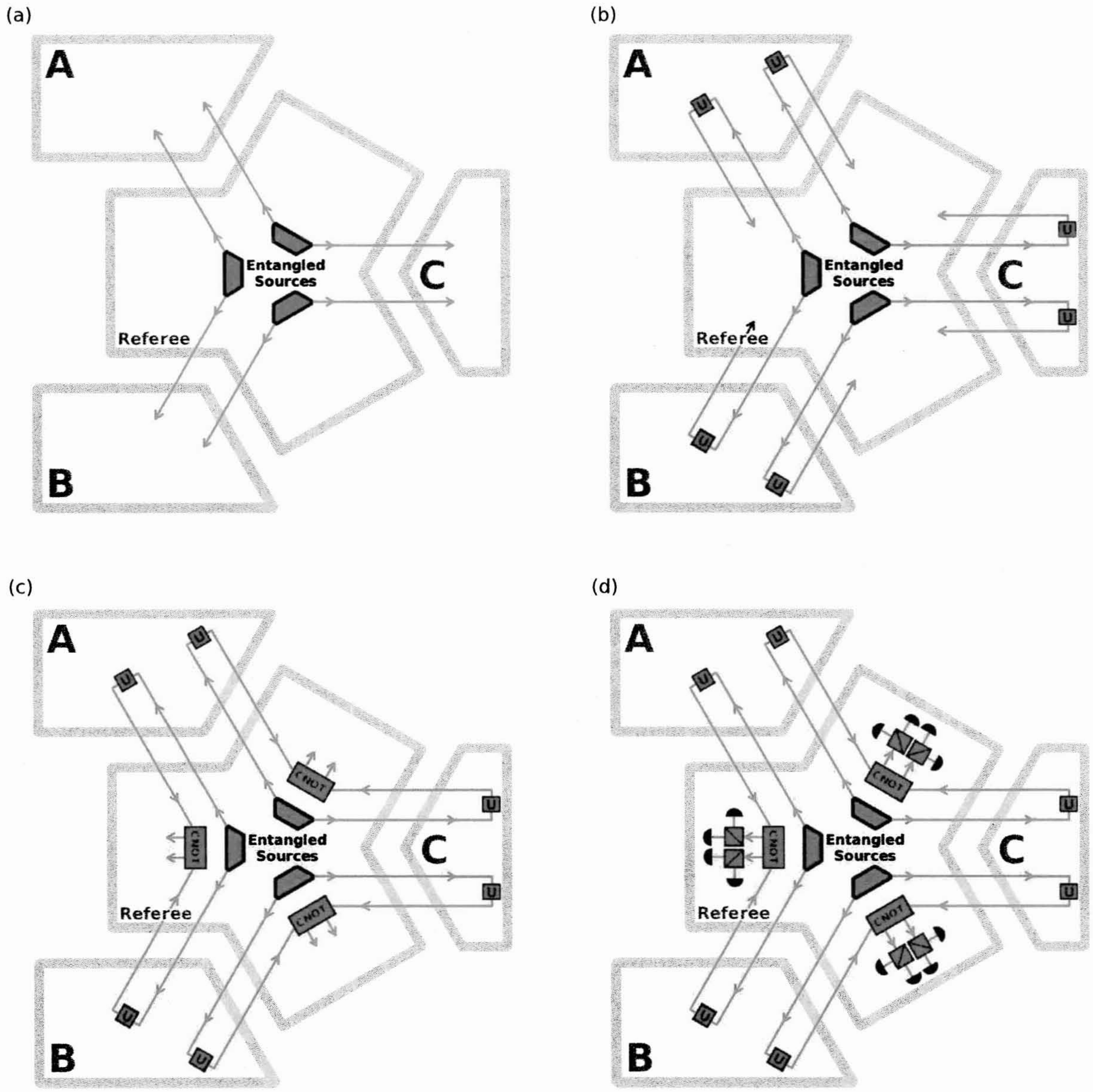

Figure 1: Experimental steps in the 3-player quantum public goods protocol. (1) The referee distributes entangled photon pairs to players A, B, and C. Each player shares one half of an entangled pair with each of their nearest neighbors. (2) Players perform quantum operations on the two photons they control and return the photons to the referee. These quantum operations implement each player's strategy. (3) The referee applies an entangling operation, equivalent to a CNOT gate and a basis transformation, to each of the photon pairs. (4) A measurement is made on each photon. If either of a player's photons is measured in the "0" state, that player is required to contribute. If both of a player's photons are measured in the "1" state, that player defects (does not contribute).

Another variation in the protocol allows partial contribution per player. In this variation, each of a player's qubits that are measured represent a fraction of that player's contribution, so in the case shown in Figure 1, a player contributes nothing if both of his/her photons are measured in the "1" state, contributes $\frac{1}{2}$ if one photon is measured in the "1" state and one photon is measured in the "0" state, and contributes 1 if both photons are measured in the "0" state. The expectation per player for all of these variations is summarized in the following table:

	Full Contribution	**Partial Contribution**
Nearest Neighbor Entanglement	$(1+3a)/4$	$(1+a)/2$
Full Pairwise Entanglement	$a-2^{-(n-1)}(a-1)$	$(1+a)/2$

The strategies that lead to these equilibria are mixed, in other words, the players probabilistically choose between two unitary transformations when acting on their photonic qubits. In practice this could be performed with quickly varying electro-optic modulators, or for our proof-of-principle experiment, by changing the setting of a wave plate or fiber polarization controller from one run of the experiment to another. A general proof of the equilibrium expectations per player cited above can be found in [1].

It is important to note that [1] also discusses the use of "full entanglement", i.e., a quantum state that represents simultaneous entanglement between every player, instead of many bipartite entangled states as in the above algorithm. Full entanglement, while theoretically convenient, is prohibitively difficult to implement experimentally. It is the fact that this algorithm requires only bipartite entangled states what makes it feasible to implement, and a key focus of a larger program in quantum games will be to develop algorithms which require only bipartite entangled states, as it is feasible to reliably produce these types of photon pairs in large quantities.

2.3 Proposed Research

A practical quantum public goods protocol has the potential to mitigate the free-rider problem, rewarding individual participation in consensus-based decision making. A practical quantum auction protocol has the potential to increase government revenue by allowing more complicated and secure bidding strategies. Here we proposed to build an experimental system which demonstrates that the implementation of quantum games is currently feasible. To that end, we proposed to build and characterize a proof-of-principle experiment which demonstrates that a quantum public goods game is feasible.

In addition, we proposed to carry out simultaneous theoretical investigations. These included: Analyzing the quantum public goods game presented here; designing a blueprint for the development of a practical quantum auction protocol; investigating how quantum protocols can add security to competitive situations; and analyzing the feasibility of running multi-party quantum games over metro-distance optical fiber.

3 LOQC-compatible Source of Entangled Photons

We have constructed and experimentally characterized the first fiber-based source of degenerate, polarization-entangled photon pairs in the telecom band. Our source design utilizes an optical-fiber Sagnac loop that is pumped with bichromatic pump pulses and aligned to deterministically separate the degenerate photon pairs. The source exhibits 0.96 ± 0.01 fidelity with a maximally entangled state, measured using quantum state tomography, and a HOM interference visibility of 0.97 ± 0.04 when configured to produce identical photon pairs.

3.1 Experimental Configuration

Photon pairs can be generated in optical fibers by means of the spontaneous four-wave mixing (FWM) process [2], wherein two pump photons scatter, while conserving energy and momentum, to create a pair of time-energy entangled daughter photons (historically called the signal and idler photons). Using a dual-frequency pump, frequency-degenerate pairs are created that are indistinguishable in all degrees of freedom: spatial mode, temporal profile, and polarization. Because the daughter photons in the degenerate case populate *exactly* the same total mode, their deterministic separation into distinct spatial modes is a challenge that this source was built to overcome.

Degenerate photon pairs are deterministically separated into distinct spatial modes when they are created in a Sagnac-loop-based "quantum splitter" topology. This configuration consists of a 50/50 fiber coupler, a piece of dispersion-shifted fiber used as the non-linear medium, and a fiber polarization controller (FPC). This type of optical fiber Sagnac loop (OFSL) is a well-known tool in optics [3]; by controlling the unitary rotation performed by the FPC, it is possible to cause all input light to the OFSL to be either totally transmitted or totally reflected. By choosing a middle ground in partially transmissive, partially reflective domain, and setting the phase between the clockwise and counter-clockwise spatial modes using FPC, reverse Hong-Ou-Mandel interference guarantees that exactly one daughter photon is emitted into each output spatial mode [4]. This alignment of the FPC is done by minimizing directly measured probability that generated photon pairs bunch in the same spatial mode when exiting the OFSL. The pair bunching probability is measured directly using a 50-50 coupler to split one output of the OFSL and collecting bunched-pair-originated coincidence counts between the two outputs of the 50-50 coupler, as well as split-pair-generated coincidence counts between the other OFSL output and either output of the 50-50 coupler.

A dual-wavelength, diagonally polarized pump pulse ($|D_p^{(\omega_1,\omega_2)}\rangle$) spontaneously four-wave mixes into two co-polarized, spatially separated, central-wavelength signal ($|D_s\rangle$) and idler ($|D_i\rangle$) photons through the following process: $|D_p^{(\omega_1,\omega_2)}\rangle \rightarrow |D_s\rangle|D_i\rangle$, where $|D_j\rangle \equiv (|H_j\rangle + |V_j\rangle)/\sqrt{2}$, for $j = s, i$. Note that these photon pairs are time-energy entangled, but not polarization entangled.

Our source, shown in Figure 2, exploits this process to create degenerate-frequency polarization entanglement. Entanglement generation requires that a distinguishing degree of freedom be coupled to the pump polarization before spontaneous four-wave mixing and that this distinguishing information be subsequently erased, causing pairs of orthogonally-polarized photon-pair amplitudes to superpose. Consider the diagonally polarized pump pulses $|D_p^{(\omega_1,\omega_2)}\rangle$. After a polarization dependent time delay t', the pump state can be described by $(|H_p^{(\omega_1,\omega_2)}\rangle \otimes |t+t'\rangle + |V_p^{(\omega_1,\omega_2)}\rangle \otimes |t\rangle)/\sqrt{2}$. Degenerate pair production (from reverse Hong-Ou-Mandel interference between the spontaneous four-wave mixing amplitudes) is then described by $|H_p^{(\omega_1,\omega_2)}\rangle \otimes |t+t'\rangle + |V_p^{(\omega_1,\omega_2)}\rangle \otimes |t\rangle \rightarrow |H_s H_i\rangle \otimes |t+t'\rangle + |V_s V_i\rangle \otimes |t\rangle$. By subjecting these degenerate photons to a second and complementary polarization-dependent time delay

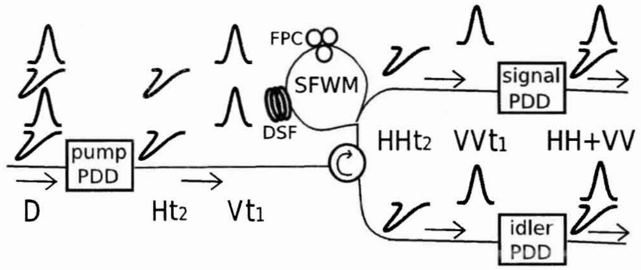

Figure 2: Polarization entanglement generation. Dual-wavelength diagonally polarized pump enters pump PDD where horizontal pump component is slid behind vertical in time by 1.12 ns. The pumps enter the non-linear medium in state $|H\rangle|t_2\rangle + |V\rangle|t1\rangle$ at each wavelength and generate photon pairs in state $|HH\rangle|t_2\rangle + |VV\rangle|t_1\rangle$ at the central wavelength. We then slide the polarization components back in time in signal and idler PDDs and get the maximally entangled state $|HH\rangle + |VV\rangle$. SFWM - spontaneous four-wave mixing; DSF - dispersion-shifted fiber; FPC - fiber polarization controller in the Sagnac loop.

we produce the maximally entangled state $2^{-1/2}(|H_sH_i\rangle + |V_sV_i\rangle) \otimes |t\rangle$.

Experimentally, we create each polarization-dependent time delay (PDD) by using free-space optical delay lines and a polarizing beam splitter in a Michelson configuration. An alternative method for achieving temporal separation and recombination of polarization components uses polarization maintaining (PM) fibers cut to identical lengths [5]. Note that the polarization-dependent time delays in this degenerate entangled-pair creation scheme are exactly analogous to the polarization-dependent spatial-mode couplings and decouplings in the counter-propagating scheme for non-degenerate entangled-photon-pair production [6].

The experimental setup has two main parts: pump preparation and the entanglement source. Dual-wavelength pump pulses are obtained by spectrally carving the output of a femtosecond laser. The detailed arrangement is similar to that in Ref. [4]. Before the pulses enter the pump PDD, using a fiber polarization controller, the pump polarization is set to diagonal with respect to polarizing beam splitter at the pump PDD input. The horizontal component of the dual-wavelength pump pulse emerges from the PDD delayed by 1.12 ns relative to the vertical component. The temporal overlap of the two pump wavelengths' pulses is controlled using a translation stage in the second pump filter.

In the experimental setup of the entanglement source, the Sagnac loop is preceded by a circulator, which redirects photons reflected by the Sagnac loop to the idler output spatial mode. Spontaneous Raman scattering in the dispersion-shifted fiber is suppressed by cooling the fiber to 77 K using liquid nitrogen [7]. Separate signal and idler polarization PDDs in the output paths superpose the orthogonally polarized FWM amplitudes. The degenerate FWM photons are then selected by two optical bandpass filters. The filtered signal and idler photons pass through polarization analyzers and are detected using four single-photon detectors (NuCrypt LLC, Model SPD 1000) made with gated InGaAs avalanche photodiodes. The detection rate was 8.3 MHz and the average dark-count probability for the four detectors was 3×10^{-4} per pulse. To make sure the polarization bases are overlapped in all PDDs, the polarizations incident on the signal and idler PDDs are adjusted using their input waveplates such that the three output pulses, observed on an oscilloscope, merge into one (the components that are twice delayed or twice advanced are eliminated). The PDD delay is set to 1.12 ns, in order to slide the small cross-polarized FWM component out of the 1 ns-wide detection window. To ensure that the path difference between PDD arms is the same in all three PDDs (to within a tenth of a picosecond), we use optimization by degree of polarization. By passing pulsed light through two PDDs in sequence onto a polarimeter, one can use translation stages in the PDD arms to maximize the output degree of polarization, which sensitively depends on the time overlap of the horizontally and vertically polarized pulses.

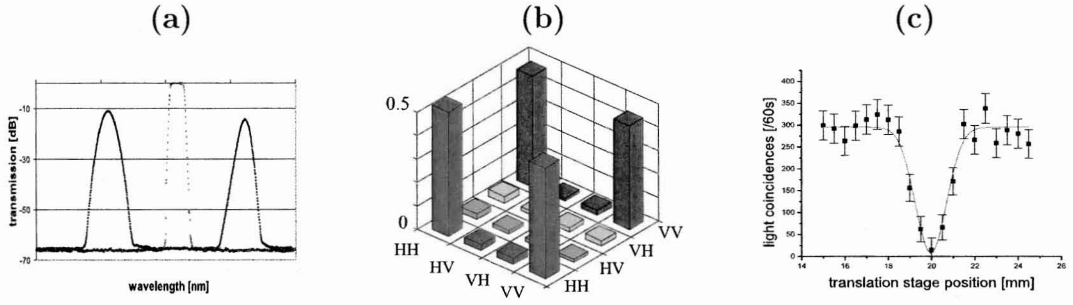

Figure 3: (a) Filter spectra. Diffraction grating filter spectra for dual-wavelength pumps (blue) and optical band pass filter spectra at the signal and idler wavelength (pink). Pump central wavelengths are 1546 nm and 1556 nm, pulse width $\simeq$ 5 ps, FWHM $\simeq$ 0.6 nm for each passband. The center (signal/idler) wavelength is 1550.92 nm, passband $\simeq$ 0.8 nm. (b) Absolute value of the reconstructed density matrix of generated polarization entangled state close to $|HH\rangle + |VV\rangle$. Collected over 8×10^7 detector gates at detection rate of 8.3 MHz. (c) Measured Hong-Ou-Mandel dip (dots) and Gaussian fit (red line). Shown are the coincidence counts vs translation stage setting which controls time of arrival of photons to the 50/50 coupler. Counts were collected for 60 s at detection rate of 785 kHz at average pump power 100μW entering the nonlinear fiber spool. The displayed coincidence counts exclude dark count-generated coincidence counts.

3.2 Source Characterization

We characterize the degenerate pholarization entangled source in two ways. The degeneracy is tested by means of Hong-Ou-Mandel interference and the entanglement via quantum state tomography. Tomographic state reconstruction requires experimentally projecting the polarization state of the photon pair into a certain number of known states (in our case thirty-six states [8]) using the polarization analyzers (consisting of a quarter-wave plate, a half-wave plate and a polarizing beam splitter). For each setting of the polarization analyzers' waveplates (corresponding to one measurement configuration), photon counts are collected at all four output ports of the signal and idler arm polarizing beam splitters. When two detectors fire in the same triggered time slot, we call the event a "coincidence" count. The collected coincidence counts in the thirty six measurement configurations are fed to a maximum likelihood tomography algorithm which finds the physical density matrix most likely to have produced the measured data [9].

The reconstructed density matrix of the polarization state of the generated photon pairs is shown in Figure 3b. Its "general Bell fidelity" [10] is $F = 0.96 \pm 0.01$, tangle [11] $T = 0.84 \pm 0.03$ and linear entropy [11] $S_{LIN} = 0.10 \pm 0.02$. Output state quality is sensitive to any timing information which distinguishes the pair's polarization components. Preliminary studies show that polarization maintaining (PM) fibers may provide even greater precision than the current free-space PDD designs. The PDD PM fibers would also avoid another obstacle: the free-space PDD setup is vulnerable to phase stability changes due to air currents (which have been minimized by constructing enclosures around the PDDs).

A high HOM interference visibility ensures that photon pairs are in identical spatiotemporal modes [12]. To check the spatial and time-frequency mode overlap of the pairs, we fixed the polarization mode of the photons by using single-polarization dual-wavelength pump. In a slightly modified experimental setup, the generated co-polarized signal and idler photons each pass through a free-space optical delay line (for variable delay) with a polarizer and a pair of waveplates (for polarization overlap control), and through an optical band pass filter (to reject the pump photons). Then the photons meet on an in-fiber 50-50 coupler (i.e., a beam splitter) where the HOM interference takes place. The output ports of the 50-50 coupler are sent to two custom avalanche photodiode single photon counters for coincidence detection. The HOM experiment is performed by measuring the coincidence count rate as a function of the relative time delay between the signal and idler photons (equivalent to the overlap between the two identical photon wave-packets).

The measured HOM dip is shown in Figure 3c. Only dark count-induced coincidences were subtracted from the directly measured coincidence counts [13]. The dip visibility, defined as the ratio of dip depth and offset, is 0.97 ± 0.04. We have measured separately the background of coincidences that mainly amount for the remaining 3%. They occur when two photons come down signal path together and split at the 50-50 coupler half the time to give a coincidence count, combined with such contribution from two photons coming down idler path. These occurrences of more than one photon per arm are primarily due to multipair generation (higher order terms in FWM) and a remaining small probability of photon pairs bunching at the Sagnac loop output, due to imperfect Sagnac's FPC adjustment in setting the reverse HOM operation at the Sagnac loop 50-50 coupler.

4 The Quantum Controlled-Not Gate

An entangling, two-qubit operation is necessary to implement the quantum public goods game. Here we use the controlled-NOT (CNOT) gate as our maximally entangling operation, operating in the polarization basis. In the process of characterizing our CNOT gate, we developed a technique for analyzing the CNOT gate in its single-photon operational basis that we then used to compensate for systematic errors in the measurement setup. To explain this compensation technique, we first review in detail the operation of the CNOT gate, whether used with single-photon inputs or two-photon inputs.

4.1 The CNOT operator

Entangling gates are a fundamental primitive for scalable quantum information processing [14]. The CNOT gate is an example of a maximally entangling gate which allows the state of one qubit (the 'control' qubit) to conditionally flip the state of another qubit (the 'target' qubit). In the two-qubit basis $\{00, 01, 10, 11\}$ (the first digit denotes the value of the control, the second the value of the target), the CNOT gate is defined by the unitary matrix:

$$U_{\text{CNOT}} = \begin{array}{c} \\ |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \begin{array}{c} \begin{array}{cccc} \langle 00| & \langle 01| & \langle 10| & \langle 11| \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array}. \tag{5}$$

In this canonical basis, the CNOT gate appears to perform a very classical function. Its entangling character is not revealed until it operates on superposed input states. When operating on the completely separable input state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle$, the CNOT gate outputs the maximally entangled Bell state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. This entangling operation can furthermore be utilized in reverse, transforming a CNOT gate into a Bell measurement:

$$\begin{aligned} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) &\overset{\text{CNOT}}{\longleftrightarrow} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \\ \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) &\overset{\text{CNOT}}{\longleftrightarrow} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |0\rangle \\ \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) &\overset{\text{CNOT}}{\longleftrightarrow} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle \\ \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) &\overset{\text{CNOT}}{\longleftrightarrow} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |1\rangle. \end{aligned} \tag{6}$$

Each of the four maximally entangled Bell states is rotated to or from one of four separable states (which can be more easily experimentally measured or created).

This operation, while clearly very useful for quantum information processing, requires there to be a direct interaction between the two qubits. For photons, where there is no appreciable coupling between two single photons, this is a daunting requirement. In order to overcome this obstacle, Knill, LaFlamme, and Milburn proposed instead using the quantum mechanical measurement process to provide the massive nonlinearity necessary to couple two single photons [15, 16]. This computational paradigm allows nondeterministic but scalable two-photon gates to be created using only linear optics.

4.2 Implementing the CNOT using linear optics

Linear optics quantum computing (LOQC) [15, 16] is a quantum information processing paradigm which relies solely on linear optical elements and single-photon counters to achieve scalable computation. The LOQC CNOT gate described here, for example, acts exactly as a standard quantum CNOT gate, except that it is only successful 1/9 of the time, where success is defined by exactly one photon being measured in each of the control and target outputs. This general LOQC gate can be encoded using either spatial or polarization qubits, and physical implementations for both encodings are shown in Figure 4.

The spatial and polarization encodings are equivalent, and each perform the CNOT operation outlined in Equation 5 with a success probability of 1/9. Because these gates are constructed using only linear optics, it is possible to describe their complete operation using

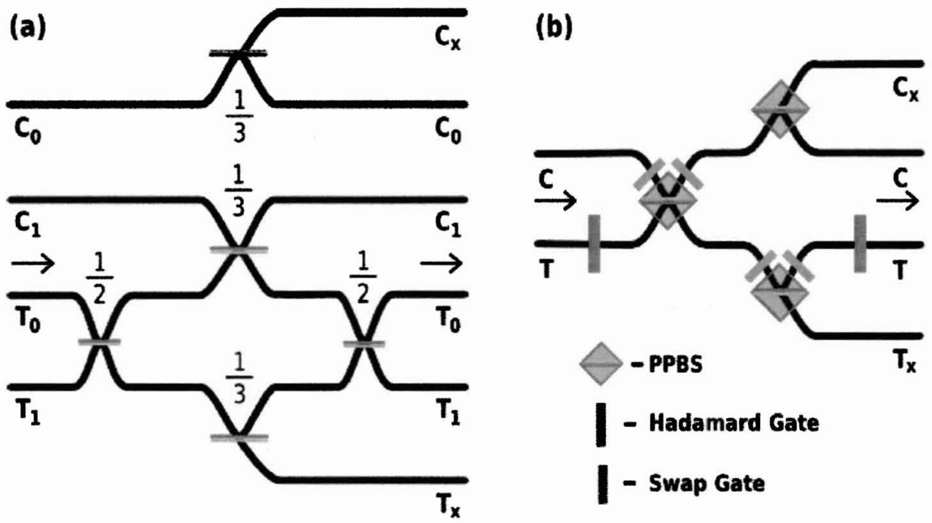

Figure 4: Pictorial diagrams of two physical implementations for a linear optics CNOT gate. (a) A spatially-encoded CNOT gate. C_0 and C_1 label the 0 and 1 modes of the control qubit, whereas T_0 and T_1 denote the canonical basis states of the target qubit. Beamsplitters are colored to indicate their reflectivity, green for $R = \frac{1}{3}$ and blue for $R = \frac{1}{2}$. In each case the grey side of the beamsplitter provides an $e^{i\pi}$ phase on reflection. (b) The same gate implemented using two polarization-encoded qubits. Here the horizontal and vertical polarization states define the logical qubit basis according to the rules $|0\rangle \equiv |H\rangle$ and $|1\rangle \equiv |V\rangle$. Swap and Hadamard gates can be implemented with half-waveplates at 45° and 22.5°, respectively. The partially polarizing beam splitter (PPBS) perfectly reflects vertically polarized light ($R_V = 1$) and partially reflects horizontally polarized light ($R_H = \frac{1}{3}$). The grey side of the PPBS provides an $e^{i\pi}$ phase to horizontally polarized light on relfection.

only single-photon transformations. When a single control photon and a single target photon are input to the gate, the CNOT operates on a vector space spanned by the four-element two-photon basis $\{C_0T_0, C_0T_1, C_1T_0, C_1T_1\}$. When a single photon in *either* the control or target is input, the gate operates on a vector space defined by a four-element *single-photon* basis: $\{C_0, C_1, T_0, T_1\}$, where C_i and T_i denote the control and target modes for the state $|i\rangle$. By breaking up the CNOT's operation into four steps, and tracking how these four single-photon inputs evolve at each stage, Figure 5 plots the step-by-step evolution of each single-photon input, for both the spatial and polarization encodings. Note that at every step, the spatial and polarization encodings are equivalent.

The single-photon creation operators $a^\dagger_{C_i}$ and $a^\dagger_{T_i}$ operating on the total vacuum state $|0\rangle$ describe photons which populate the modes C_i and T_i. For readability, we will refer to these creation operators through the use of the "hatted" operators $\hat{C}^\dagger_i \equiv a^\dagger_{C_i}$ and $\hat{T}^\dagger_i \equiv a^\dagger_{T_i}$. Using

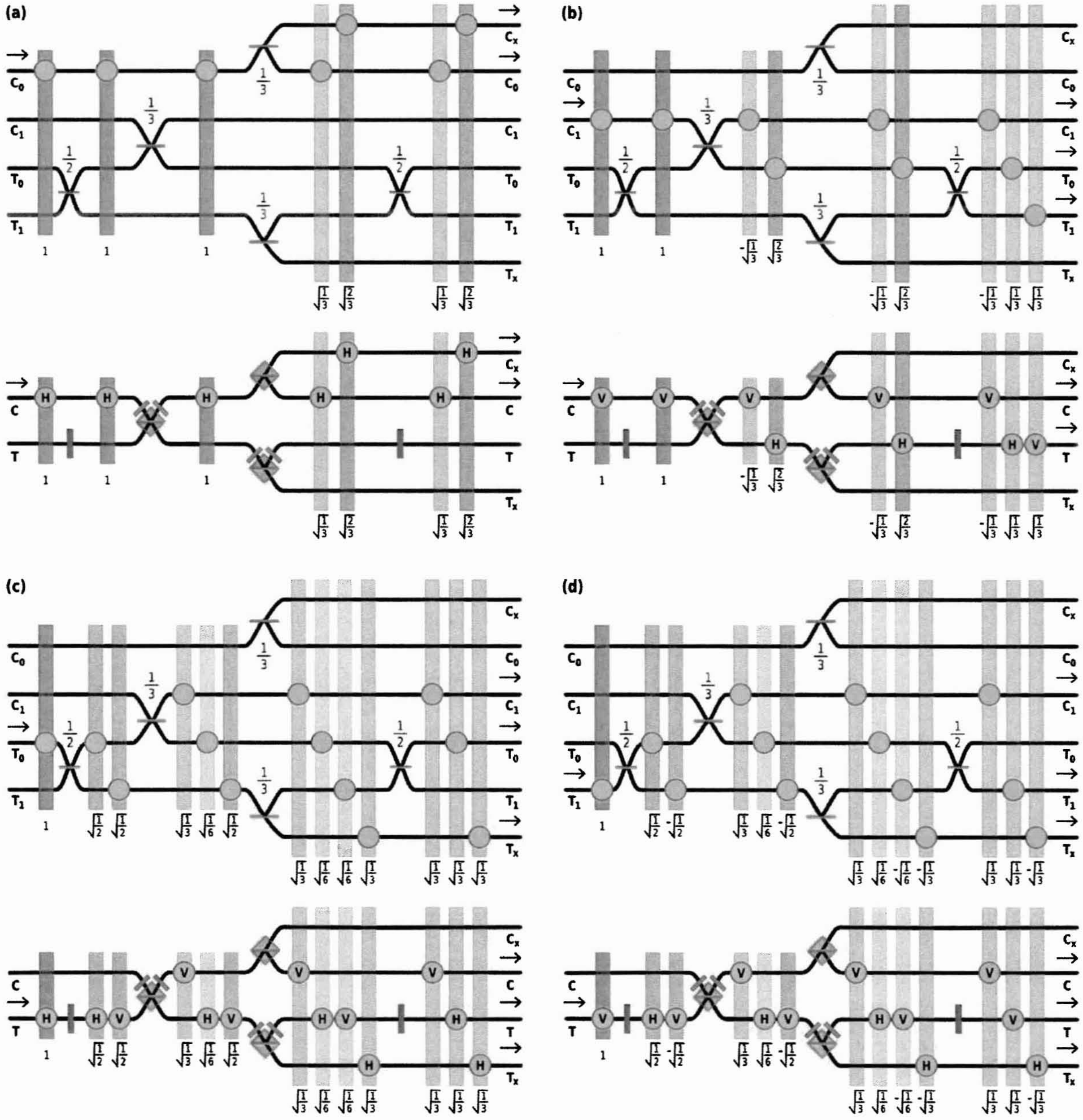

Figure 5: Graphical representation of the single-photon transformations performed by both the spatially-encoded and polarization-encoded linear optics CNOT gates. Optical elements are labelled as in Figure 1. As it travels through successive components of the gate, each photon evolves into a superposition of different spatial/polarization modes. These superposed modes are graphically depicted after each major CNOT component, with each vertical box depicting a single term of the superposition. Each box is faded in inverse proportion to its term's amplitude (the amplitude is explicitly noted below the photon). (a) Evolution of the state $\hat{c}_0^\dagger|0\rangle$ into the single-photon superposition $\sqrt{\frac{1}{3}}\left(\hat{c}_0^\dagger + \sqrt{2}\hat{c}_X^\dagger\right)|0\rangle$, and of the state $\hat{c}_H^\dagger|0\rangle$ into the single-photon superposition $\sqrt{\frac{1}{3}}\left(\hat{c}_H^\dagger + \sqrt{2}\hat{c}_X^\dagger\right)|0\rangle$. Note that these two processes are identical. (b) Evolution of $c_{1/V}^\dagger|0\rangle$ into $\sqrt{\frac{1}{3}}\left(-\hat{c}_{1/V}^\dagger + \hat{T}_{0/H}^\dagger + \hat{T}_{1/V}^\dagger\right)|0\rangle$. (c) Evolution of $T_{0/H}^\dagger|0\rangle$ into $\sqrt{\frac{1}{3}}\left(\hat{c}_{1/V}^\dagger + \hat{T}_{0/H}^\dagger + \hat{T}_X^\dagger\right)|0\rangle$. (d) Evolution of $T_{1/V}^\dagger|0\rangle$ into $\sqrt{\frac{1}{3}}\left(\hat{c}_{1/V}^\dagger + \hat{T}_{1/V}^\dagger - \hat{T}_X^\dagger\right)|0\rangle$.

this notation, the CNOT single-photon transformations are:

$$\hat{C}_0^\dagger \overset{\text{CNOT}}{\longrightarrow} \sqrt{\frac{1}{3}}\left(\hat{C}_0^\dagger + \sqrt{2}\hat{C}_X^\dagger\right) \tag{7}$$

$$\hat{C}_1^\dagger \overset{\text{CNOT}}{\longrightarrow} \sqrt{\frac{1}{3}}\left(-\hat{C}_1^\dagger + \hat{T}_0^\dagger + \hat{T}_1^\dagger\right) \tag{8}$$

$$\hat{T}_0^\dagger \overset{\text{CNOT}}{\longrightarrow} \sqrt{\frac{1}{3}}\left(\hat{C}_1^\dagger + \hat{T}_0^\dagger + \hat{T}_X^\dagger\right) \tag{9}$$

$$\hat{T}_1^\dagger \overset{\text{CNOT}}{\longrightarrow} \sqrt{\frac{1}{3}}\left(\hat{C}_1^\dagger + \hat{T}_1^\dagger - \hat{T}_X^\dagger\right), \tag{10}$$

where C_X and T_X represent creation operators for two ancillary dump modes into which input photons are probabilistically lost. In order to derive the two-photon operation for the same gate, we have only to apply the above transformations to the standard basis of two-photon inputs:

$$\begin{aligned}\hat{C}_0^\dagger\hat{T}_0^\dagger &\overset{\text{CNOT}}{\longrightarrow} \frac{1}{3}\left(\hat{C}_0^\dagger + \sqrt{2}\hat{C}_X^\dagger\right)\left(\hat{C}_1^\dagger + \hat{T}_0^\dagger + \hat{T}_X^\dagger\right) \\ &= \frac{1}{3}\Big(\hat{C}_0^\dagger\hat{C}_1^\dagger + \underline{\hat{C}_0^\dagger\hat{T}_0^\dagger} + \hat{C}_0^\dagger\hat{T}_X^\dagger + \\ &\qquad \sqrt{2}(\hat{C}_X^\dagger\hat{C}_1^\dagger + \hat{C}_X^\dagger\hat{T}_0^\dagger + \hat{C}_X^\dagger\hat{T}_X^\dagger)\Big)\end{aligned} \tag{11}$$

$$\begin{aligned}\hat{C}_0^\dagger\hat{T}_1^\dagger &\overset{\text{CNOT}}{\longrightarrow} \frac{1}{3}\left(\hat{C}_0^\dagger + \sqrt{2}\hat{C}_X^\dagger\right)\left(\hat{C}_1^\dagger + \hat{T}_1^\dagger - \hat{T}_X^\dagger\right) \\ &= \frac{1}{3}\Big(\hat{C}_0^\dagger\hat{C}_1^\dagger + \underline{\hat{C}_0^\dagger\hat{T}_1^\dagger} - \hat{C}_0^\dagger\hat{T}_X^\dagger + \\ &\qquad \sqrt{2}(\hat{C}_X^\dagger\hat{C}_1^\dagger + \hat{C}_X^\dagger\hat{T}_1^\dagger - \hat{C}_X^\dagger\hat{T}_X^\dagger)\Big)\end{aligned} \tag{12}$$

$$\begin{aligned}\hat{C}_1^\dagger\hat{T}_0^\dagger &\overset{\text{CNOT}}{\longrightarrow} \frac{1}{3}\left(-\hat{C}_1^\dagger + \hat{T}_0^\dagger + \hat{T}_1^\dagger\right)\left(\hat{C}_1^\dagger + \hat{T}_0^\dagger + \hat{T}_X^\dagger\right) \\ &= \frac{1}{3}\Big(- \hat{C}_1^\dagger\hat{C}_1^\dagger - \hat{C}_1^\dagger\hat{T}_X^\dagger + \hat{T}_0^\dagger\hat{T}_0^\dagger + \hat{T}_0^\dagger\hat{T}_X^\dagger \\ &\qquad + \underline{\hat{C}_1^\dagger\hat{T}_1^\dagger} + \hat{T}_1^\dagger\hat{T}_0^\dagger + \hat{T}_1^\dagger\hat{T}_X^\dagger\Big)\end{aligned} \tag{13}$$

$$\begin{aligned}\hat{C}_1^\dagger\hat{T}_1^\dagger &\overset{\text{CNOT}}{\longrightarrow} \frac{1}{3}\left(-\hat{C}_1^\dagger + \hat{T}_0^\dagger + \hat{T}_1^\dagger\right)\left(\hat{C}_1^\dagger + \hat{T}_1^\dagger - \hat{T}_X^\dagger\right) \\ &= \frac{1}{3}\Big(- \hat{C}_1^\dagger\hat{C}_1^\dagger + \hat{C}_1^\dagger\hat{T}_X^\dagger + \underline{\hat{C}_1^\dagger\hat{T}_0^\dagger} + \hat{T}_0^\dagger\hat{T}_1^\dagger \\ &\qquad - \hat{T}_0^\dagger\hat{T}_X^\dagger + \hat{T}_1^\dagger\hat{T}_1^\dagger - \hat{T}_1^\dagger\hat{T}_X^\dagger\Big).\end{aligned} \tag{14}$$

In each case the superposed term corresponding to successful CNOT operation has been underlined; all other terms do not have a single control photon (in mode C_0 or C_1) and a single target photon (in mode T_0 or T_1). The derivation of Equation 13 is graphically depicted in Figure 6.

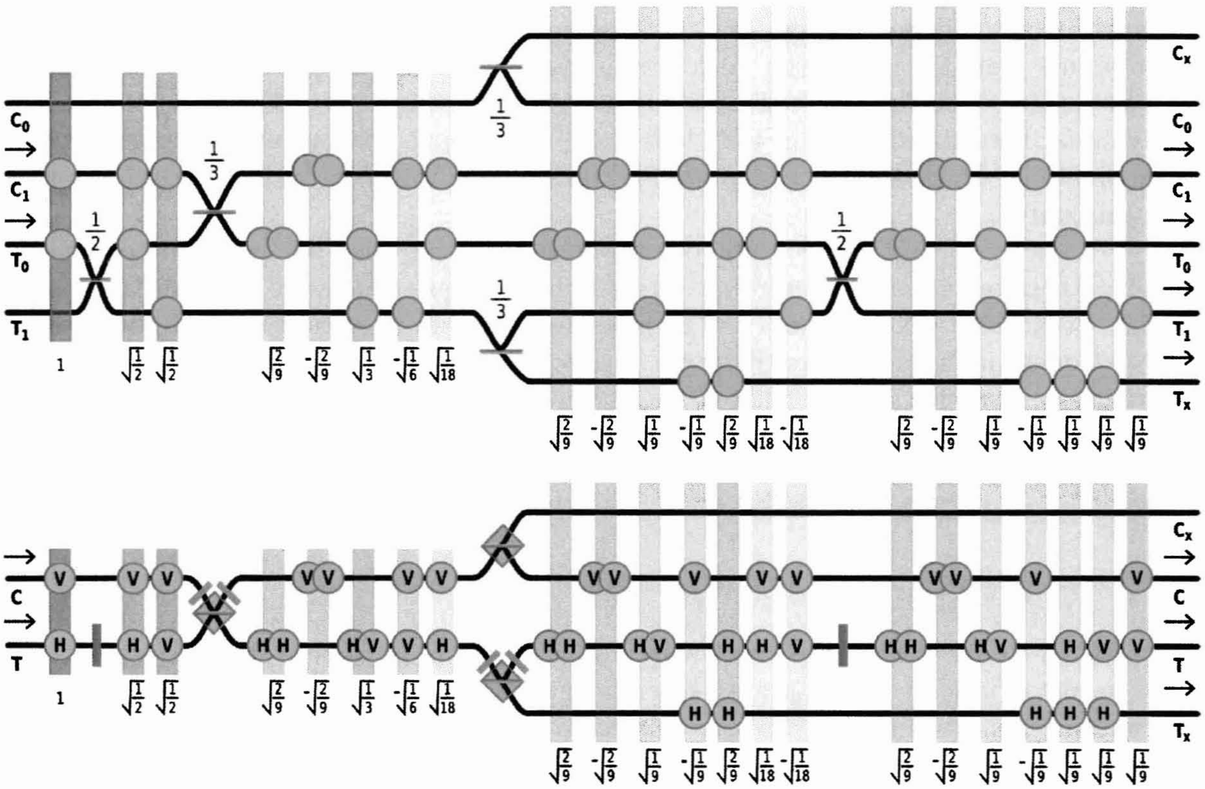

Figure 6: The operation of spatially-encoded and polarization-encoded linear optical CNOT gates on the input state $|10\rangle$, i.e., the two-photon evolution of the state $\hat{C}_1^\dagger \hat{T}_0^\dagger |0\rangle$ into the superposition state $\frac{1}{3}\Big(-\hat{C}_1^\dagger \hat{C}_1^\dagger - \hat{C}_1^\dagger \hat{T}_X^\dagger + \hat{T}_0^\dagger \hat{T}_0^\dagger + \hat{T}_0^\dagger \hat{T}_X^\dagger + \underline{\hat{C}_1^\dagger \hat{T}_1^\dagger} + \hat{T}_1^\dagger \hat{T}_0^\dagger + \hat{T}_1^\dagger \hat{T}_X^\dagger \Big)|0\rangle$. Note that this depiction uses the same style as Figure 5, except that now each superposed term is represented by a box with *two* photons. At the conclusion of the gate the two-photon state is in a 7-term superposition, only one of which represents exactly one control photon and one target photon. This term, $\sqrt{\frac{1}{3}}\left(\hat{C}_1^\dagger \hat{T}_1^\dagger\right)|0\rangle$, corresponds to a the correct CNOT output $|11\rangle$. The square of the amplitude of this term is $\frac{1}{9}$, the success probability of the linear optical CNOT gate.

4.3 Experimental layout of the CNOT gate

Once created, the degenerate input pairs are routed through single-mode fibers to the CNOT gate inputs. This telecom-band gate, although fiber-coupled, is constructed from free-space linear-optical components, and operates on spatially distinct, polarization encoded photonic qubits ($|H\rangle \equiv |0\rangle, |V\rangle \equiv |1\rangle$). The gate's central components are three custom-made partially polarizing beam-splitters (PPBSs). Each PPBS perfectly reflects incident vertically polarized light while reflecting 1/3 and transmitting 2/3 of incident horizontally polarized light. Two swap gates (half-waveplates at 45°) and two Hadamard gates (half-waveplates at 22.5°) complete the CNOT architecture, as shown in Figure 7. Note that this architecture uses two fewer swap gates than the polarization-encoded CNOT gate shown in Figures 1-3. The elements shown in the "CNOT Gate" section of Figure 7 therefore perform a different—

yet still maximally entangling—two-qubit operation; because the missing waveplates are at the inputs and outputs of the device, it is possible to use adjacent input waveplates or measurement waveplates to compensate, in effect achieving perfect CNOT operation while relying on fewer total components. It is these same input and output waveplate/polarizer combinations which allow the creation and measurement of arbitrarily polarized input and output states.

Vibrations on one of the input or output steering mirrors (not pictured) can cause a global phase on either the control or target qubit, a phase which will naturally fluctuate in time. Because all CNOT inputs and outputs are joint two-photon control-target states, the CNOT operation is immune to this noise. However, noise from the stray pump—which passes through what is effectively a huge Mach-Zender fiber-interferometer bounded by the Sagnac loop and PPBS_1—*is* affected by this time-varying phase. In order to ensure phase-averaging over any stray pump light that reaches the gate, a slowly varying (at 8 Hz) piezoelectric transducer was affixed to a target input steering mirror.

4.4 CNOT gate characterization

In order to completely characterize a two-qubit quantum process, it is necessary to record the results of at least 256 separate measurements. In practice, this many measurements can be inconvenient, or in some cases, prohibitively difficult. Luckily, it is possible to use only 32 polarization measurements to bound the total process fidelity of any two-qubit gate [17]. This bound is given by

$$\overline{F}\left(B_1\right) + \overline{F}\left(B_2\right) - 1 \leq F\left(\chi\right) \leq \min\left[\overline{F}\left(B_1\right), \overline{F}\left(B_2\right)\right], \tag{15}$$

where $\overline{F}\left(B_i\right)$ is the average fidelity of the experimental results with theoretical expectations when using the basis B_i for both the inputs and the outputs of the CNOT gate. (In the experimental characterization which follows, $B_1 = \{HH, HV, VH, VV\}$ and $B_2 = \{DD, DA, AD, AA\}$, where D and A denote diagonally and anti-diagonally polarized light, respectively.) In other words, the bounds of the fidelity of an experimental process can be obtained by measuring two complementary 16-element datasets.

After measuring the CNOT gate's performance in these two canonical bases, we obtain the average fidelities $\overline{F}\left(B_1\right) = 88.6 \pm 0.3\%$ and $\overline{F}\left(B_2\right) = 89.1 \pm 0.3\%$. The measured truth tables for these two bases are shown in Figure 8. These results bound the process fidelity between 77.7% and 88.6%. These results, while confirming the measured gate's entangling character, are clearly being limited by systematic rather than statistical errors. Studying Figure 8, one observes side-peaks, up to 10% of the height of the main peak.

We examined several potential sources of error, including multipair-production from the source and imperfect optics in the setup. Although previous CNOT characterization has been limited by the four-photon production from the source, this cause of systematic error had been largely eliminated in this experiment by lowering the pump power until four-photon events were directly measured to account for less than 5% of FWM events, limiting the probability of any multipair-induced errors to $< 2.5\%$ [18].

Inaccurately aligned and imperfect optical elements (such as waveplates and beam splitters) were another potential source of error. To estimate the contribution of optics imperfections to the total error, we used classical 1550-nm light (Santec TSL-210) as the horizontal

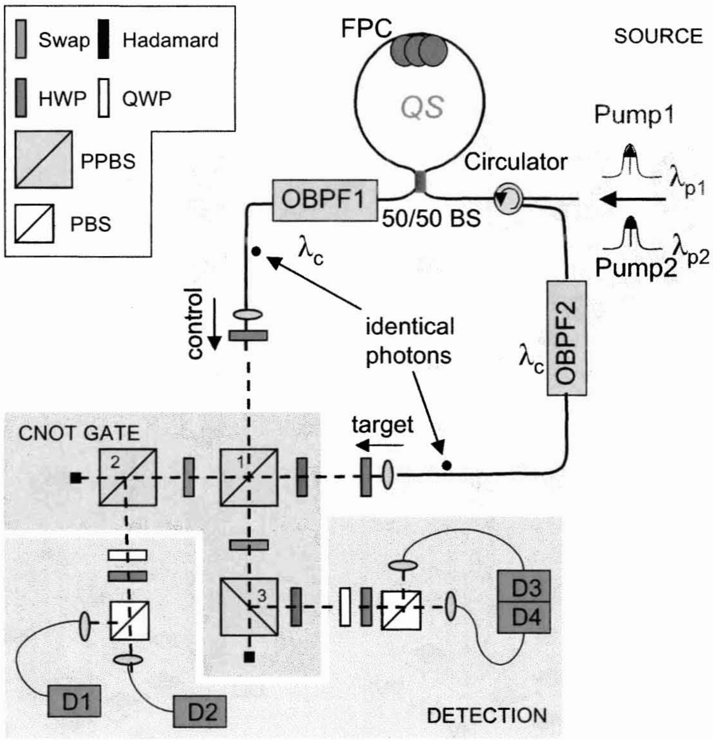

Figure 7: Experimental layout of the source connected to the CNOT gate. The two pumps, designated as pump1 and pump2 enter the Sagnac loop where they produce degenerate frequency pairs via four-wave mixing. These pairs form the *control* and the *target* input to the CNOT gate, which meet at the first partially polarizing beam-splitter (PPBS1). In the CNOT gate, PPBS1 is followed by swap gates in the two paths, which are followed by two more PPBSs, PPBS2 and PPBS3, in each arm. The measurement apparatus consists of a half-wave plate, a quarter-wave plate and a polarizing beam-splitter in each arm followed by the single photon detectors D1, D2, D3 and D4.PPBS, partially polarizing beam splitter; PBS, polarizing beam splitter; HWP, half wave plate; QWP, quarter wave plate; OBPF, optical band pass filter; QS, quantum splitter; BS, beam splitter.

control, vertical control, horizontal target, and vertical target inputs, measuring the output intensity at the each of the four output modes for each of these four inputs. This provided a direct measurement of the absolute-squares of the amplitude terms in Equations 7–10.

Using these directly measured values in conjunction with the above equations for single-photon evolution, we were able to predict exactly which truth table side-peaks could have been caused by optics imperfections. From these calculations, we determined that optics imperfections of the type we measured accounted for non-zero probabilities in the *In:VV/Out:VV*, *In:VH/Out:VH*, *In:AA/Out:AA*, and *In:DA/Out:DA* elements of the truth table, but did not account for the other eight non-zero elements.

Again turning to the single-photon-transformation picture of the CNOT gate, we noted that the remaining errors were consistent with *bunched* photon inputs, i.e., when two photons instead of one are present in a control or target input. As an example, consider the case

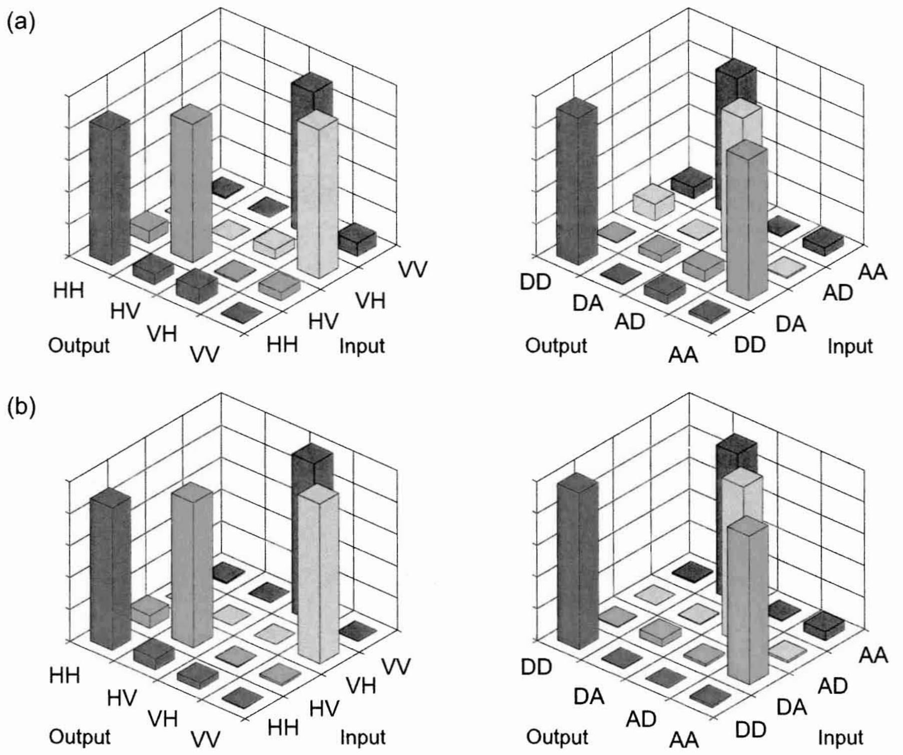

Figure 8: Experimentally measured truth tables characterizing the output of the CNOT gate. (a) The truth tables without correction for bunching in the H/V and D/A bases ($|D\rangle \equiv \sqrt{\frac{1}{2}}(|H\rangle + |V\rangle)$, $|A\rangle \equiv \sqrt{\frac{1}{2}}(|H\rangle - |V\rangle)$). The average truth table fidelity was 88.6 ± 0.6% and 89.1 ± 0.3% for the H/V and D/A bases respectively. (b) The same data after correction for bunching. After subtracting bunched coincidence counts, the average H/V fidelity was 94.8 ± 0.4% and the average D/A fidelity was 95.9 ± 0.4%. Imprefect alignment causes the degenerate photon-pair source—with small probability—to produce two photons in the control or two photons in the target, i.e., bunching. Systematic errors in coincidence rates due to this bunching effect can be directly measured by blocking either the control or target input, and then subtracted in order to reconstruct the true CNOT gate performance.

where two vertically polarized target photons and no control photons are injected into the CNOT gate. Using the single-photon transformations given in Equation 10:

$$\begin{aligned}\hat{T}_V^\dagger \hat{T}_V^\dagger |0\rangle &\xrightarrow{\text{CNOT}} \frac{1}{3}\left(\hat{C}_1^\dagger + \hat{T}_1^\dagger - \hat{T}_X^\dagger\right)\left(\hat{C}_1^\dagger + \hat{T}_1^\dagger - \hat{T}_X^\dagger\right)|0\rangle \\ &= \frac{1}{3}\left(2\hat{C}_1^\dagger \hat{T}_1^\dagger + \dots\right)|0\rangle, \end{aligned} \tag{16}$$

we can see that any bunched target vertical photons will lead to extraneous coincidences between vertical control photons and vertical target photons; these correspond to one of the sidepeaks in Figure 8(a) which remains unaccounted for. After following similar derivations for other types of bunched inputs, we found that all remaining sidepeaks could be explained through bunching effects.

Physically, this bunching phenomenon is an artifact of an imperfectly aligned Sagnac loop in the degenerate photon source (even in the 50/50 configuration, if the quantum splitter's counterclockwise and clockwise FWM components are not aligned to have identical polarizations, imperfect splitting will occur). Although these bunched photons are directly measured and minimized during source characterization, drift can still lead to some bunched photons during gate measurement. Luckily, this source imperfection can be directly measured and compensated for during the gate characterization.

To directly measure the coincidence counts due to photon bunching, we measure the output coincidence counts when either the target or the control arm is blocked (in addition to the standard measurement with both unblocked). By subtracting these bunching-induced-coincidences, we can directly measure our gate's performance if it had been supplied with perfect input states. Figure 8(b) shows the Hofmann characterization of the CNOT gate after subtraction of bunched coincidences. The compensation results in truth table fidelities of $\overline{F}\,(B_1) = 94.8 \pm 0.4\%$ and $\overline{F}\,(B_2) = 95.9 \pm 0.4\%$, which bounds the process fidelity to between 90.7% and 94.8%.

5 Four-detector Coincidence Counting Array

Fast, efficient detection is crucial for any LOQC gate characterization as well as for tomographic state reconstruction. The quantum state tomography requires efficient data collection as coincidence counts are measured in thirty-six projection states of the photon pair polarization [8]. LOQC gates are inherently non-deterministic (this CNOT gate has a 1/9 probability of success); coupled with the general lack of high-efficiency telecom-band single photon counters, this dictates that adequate detection systems are a key experimental concern. Previous experiments [18] addressed this problem by using a single superconducting single-photon detector to herald an InGaAs/InP photodiode with a gate rate of 0.8 MHz. Here we have greatly improved the total detection system by installing an array of four single-photon detectors (Nucrypt LLC, Model SPD 1000) to characterize the CNOT gate. These detectors were set to an average dark count rate of 3×10^{-4} per pulse and an operating rate of 8.3 MHz. By using an array of four detectors, we can simultaneously measure the complete four-element coincidence basis, increasing our effective data-collection rate by a factor of 4, as well as automatically compensating for any pump intensity fluctuations. Because our coincidence counts were measured using four different pairs of detectors, we used direct measurements and an in-situ maximum-likelihood program to compensate for both differences in individual detector efficiencies and output polarizing beam-splitter crosstalk. The ten-fold increase in detection rate and four-fold increase in collection rate resulted in a total data-rate 40 times faster than the previous experiments.

6 Implementing the Quantum Game

6.1 Experimental Configuration

The experimental configuration for the nearest neighbor quantum game is shown in Figure 1(d). In order to perform an experimental demonstration of this quantum game for large numbers of players, we implemented a single nearest-neighbor interaction and characterized it's results. Each nearest-neighbor interaction consists of a single entangled pair generation, two unitary operations performed by each of the two neighboring players, and finally an entangling gate followed by a four-detector measurement. By performing this measurement in sequence for each set of nearest-neighbors, it is possible to run an arbitrarily large game with a single experimental setup.

The major experimental components for this device have already been described. Section 3 described the LOQC-compatible entangled photon source. Section 4 detailed the entangling gate. Section 5 described the four-detector array. The unitary transformations which encoded each player's "move" were implemented using groups of waveplates which together performed the Pauli rotations $X \equiv \sigma_X$ and $Z \equiv \sigma_Z$ and the identity I. As shown in [1], the classical game can be recreated if the players always choose I or X, corresponding to defection or contribution, respectively. In the quantum game, the ideal player strategy is to use is mixed, with an equal probability of performing either the Z or I operation on each move.

6.2 Final Experimental Results

Experimental operation of the quantum game was verified using two separate methods. First, all canonical classical and quantum game operations—pairwise combinations of I, X, and Z—were independently tested to verify that the game system as a whole behaved as expected. For the classical game, this required verifying that the operations I and X allowed a player to reliable 'contribute' or 'defect', respectively. Figure 9(a) shows the truth table for these choices. The truth table has an $82 \pm 4\%$ fidelity with theory.

For the quantum game, there are no operations which can directly be interpreted as contribution or defection, instead the optimal strategy makes use of a equal probabilistic combination of the operations I and Z. When two neighbors choose the same operation, they both defect. When they choose different operations, they both contribute. Figure 9(b) shows the truth table for the canonical quantum operations. This truth table has a $77 \pm 4\%$ fidelity with theory.

Although these fidelities are not ideal, one advantage of this particular quantum game is it's insensitivity to operational errors. Figure 10 shows the final game results for the nearest-neighbor-type quantum public goods game with $\frac{a}{n} = \frac{1}{2}$ and $c_k = 1$. Ideal curves for both classical expectation ($E_k = 1$) and quantum game expectation ($E_k = \frac{2+3n}{8}$) are shown as a function of the number of players, n. Regardless of the size of the game, the experimentally measured game results are within error of the ideal quantum game performance. The quantum over classical advantage grows linearly with number of players.

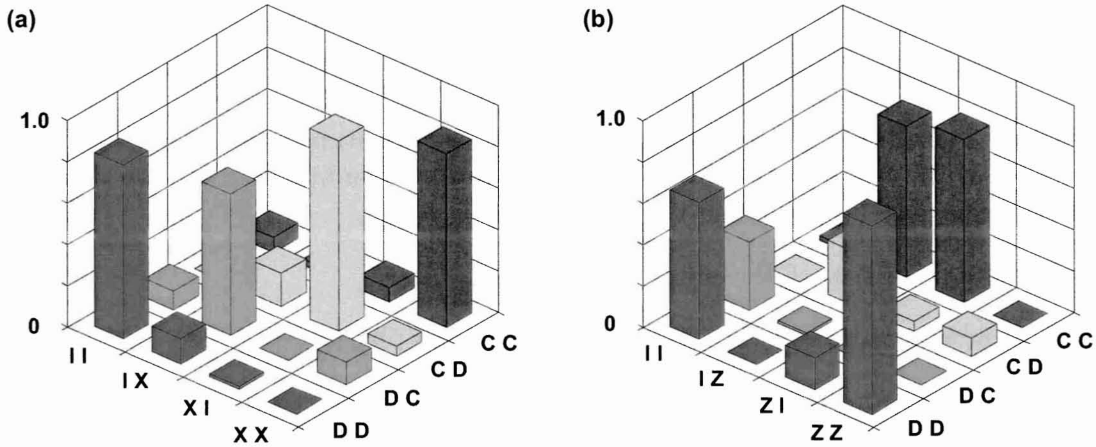

Figure 9: The operation of the quantum public goods game given canonical classical and quantum operational inputs. Bar graphs show the probabilities for different contribution/defection outcomes according to different player operations. C and D denote player contribution and defection, respectively. I, X, and Z denote the operations σ_X, σ_Y, and σ_Z, respectively. In a full, multi-player quantum game, these choices and results would apply to each pair of adjacent players. (a) Results for the 'classical' moves in the quantum public goods game. (b) Results for the 'quantum' moves in the quantum public goods game.

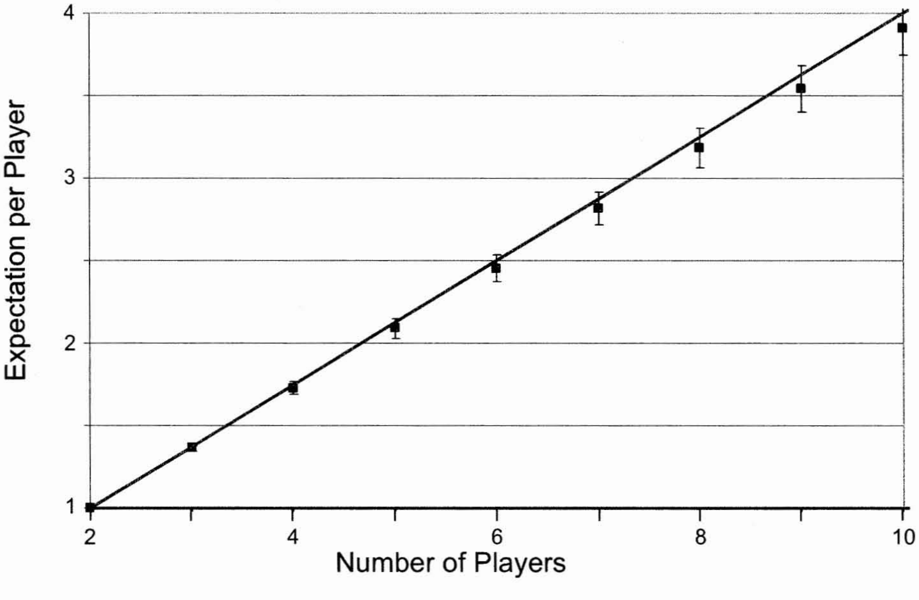

Figure 10: Experimental results for the multiplayer quantum game. Experimental data is used to simulate a multiplayer quantum game where nearest neighbors share entanglement. For the game where $\frac{a}{n} = \frac{1}{2}$, the quantum expectation per player is given by $E_k = \frac{2+3n}{8}$ (shown on the graph as the pink line). The classical expectation per player for the same game is $E_k = 1$ (shown on the graph as a blue line). All experimental data points are within error of the ideal expectation per player.

7 Theoretical Results

7.1 Formalization

We began this project by formalizing a notion of "quantum game" that includes many of the quantum protocols that have been proposed, including the one we demonstrated experimentally. A classical game Γ consists of:

- a finite number n of players;
- a strategy space $S_i = \{0, 1, \dots, |S_i| - 1\}$ for each player i;
- a payoff function $P_i : S = S_1 \times \cdots \times S_n \longrightarrow \mathbb{R}$ for each player i.

A quantum version of Γ also requires:

- a Hilbert space $\mathcal{H}_i$ for each player i;
- a map $d_i : \{0, 1, \dots, |\mathcal{H}_i| - 1\} \longrightarrow S_i$ for each player i,

where d_i provides an interpretation of the computational basis elements of $\mathcal{H}_i$ as pure strategies for player i.

Eisert, Wilkens and Lewenstein (EWL) [19] and Marinatto and Weber (MW) [20] "quantum games" should be thought of as games with quantum communication [21]. They, and the quantum public goods game of Chen, Hogg and Beausoleil [22], are each instances of the following quantum communication protocol:

1. A *referee* prepares a quantum state $\rho \in \mathcal{H} \otimes \mathcal{H}^\dagger$, where $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$ and ρ is known to the players;
2. The referee sends each player i the i^{th} subsystem of ρ;
3. Each player i acts upon his subsystem and returns it to the referee;
4. The referee acts by a unitary transformation V on the received state and measures it in the computational basis of $\mathcal{H}$, obtaining $|e_1 \dots e_n\rangle$. The payoff to player i is $P_i\bigl(d_1(e_1), \dots, d_n(e_n)\bigr)$.

In the EWL and MW protocols, $\mathcal{H}_i = \mathbb{C}^2$ and $d_i : |b\rangle \mapsto b$. They set $\rho = U|0\dots0\rangle\langle0\dots0|U^\dagger$, where $U = J_n := (I^{\otimes n} + iX^{\otimes n})/\sqrt{2}$ (although Marinatto and Weber also consider U which produce a less entangled initial state [20]); in the EWL protocol, $V = U^\dagger$, while in the MW protocol, $V = I$.

This quantum protocol generalizes the notion of a game with (classical) communication to allow for the communication of *quantum* information. The (standard) classical protocol is:

1. A referee "prepares" a classical probability distribution $\mu \in \Delta(S)$, the set of convex combinations of the elements of S, thought of as orthonormal unit vectors in $\mathbb{R}^S$. μ is known to the players;

2. The referee draws a sample from μ, and sends each player i the i^{th} component of the sample. This is the referee's *recommendation*;

3. Each player i acts upon his recommendation and returns some element of S_i, possibly chosen according to some probability distribution, to the referee;

4. The payoffs to the players are determined by the element of S received by the referee.

7.2 Equilibrium Concept for Quantum Games

Aumann defined μ to be a (classical) *correlated equilibrium* if no player can improve his expected payoff by *not* following the referee's recommendation, *i.e.*, returning the recommendation unchanged to the referee [23].

Notice that $\Delta(S_1) \times \cdots \times \Delta(S_n) \subsetneq \Delta(S)$, so the set of possible correlated equilibria *strictly includes* the set of possible mixed strategy equilibria for Γ. The set of *actual* correlated equilibria is a compact convex set containing the convex hull of the Nash equilibria of Γ, and can be strictly larger, *although not when the Nash equilibrium is a dominant strategy equilibrium.* (Recall that a strategy is *dominant* when it is the best strategy to play, independently of the other players' strategies.)

For this project we defined (ρ, V, d) to be a *quantum correlated equilibrium* of Γ if no player can improve his expected payoff by *not* acting by the identity on his subsystem. *Notice that in the quantum protocol we defined in the previous subsection, the players can act by any quantum operation on their own subsystem before returning it to the referee.* This is a more general protocol that is usually considered—in the work of Marinatto and Weber, and of Chen, Hogg and Beausoleil, the players are only allowed to act by convex combinations of unitary operations. Allowing more possible operations, of course, (weakly) decreases the set of quantum correlated equilibria.

7.3 Quantum Equilibria of the PUBLIC GOODS

We consider the $n = 3$ version of Chen, Hogg and Beausoleil's "quantum PUBLIC GOODS game" [22], since this is the one that we realized experimentally. The strategy spaces are $S_1 = S_2 = S_3 = \{0, 1\}$, which we think of as the players' possible contributions. The payoff functions are $P_i(s_1, s_2, s_3) = (1 - s_i) + 2(s_1 + s_2 + s_3)/3$.

The unique Nash equilibrium of this game is $s_1 = s_2 = s_3 = 0$, at which each player gets a payoff of 1. This may be contrasted with the *Pareto optimal* point, $s_1 = s_2 = s_3 = 1$, at which each player gets a payoff of 2. The latter is *not* a Nash equilibrium since player i can improve his payoff to 7/3 by unilaterally changing to $s_i = 0$.

Note that $s_i = 0$ is a dominant strategy: player i always gets a higher payoff by playing this strategy, no matter what the other players do. As we noted above, this means that there is no (classical) correlated equilibrium other than the Nash equilibrium.

In our formalization of Chen, Hogg and Beausoleil's quantum version of this game [22], $\mathcal{H}_i = \mathbb{C}^2 \otimes \mathbb{C}^2$, and the interpretation of computational basis vectors as pure strategies is:

$$d_i : |bc\rangle \mapsto \begin{cases} 1 & \text{if } b = 1 \text{ or } c = 1; \\ 0 & \text{otherwise.} \end{cases}$$

Following Chen, Hogg and Beausoleil [22], define $U = J_2^{(23)} \otimes J_2^{(45)} \otimes J_2^{(61)}$, where the superscripts indicate upon which pair of the six qubits in $\mathcal{H}$ each J_2 acts. Now let

$$\begin{aligned}\rho = 2^{-12} \sum (iZ)^{b_1} \otimes (iZ)^{c_1} \otimes (iZ)^{b_2} \otimes (iZ)^{c_2} \otimes (iZ)^{b_3} \otimes (iZ)^{c_3} \cdot U|000000\rangle \otimes \\ \langle 000000| U^\dagger \cdot (-iZ)^{b_1} \otimes (-iZ)^{c_1} \otimes (-iZ)^{b_2} \otimes (-iZ)^{c_2} \otimes (-iZ)^{b_3} \otimes (-iZ)^{c_3},\end{aligned}$$

where the sum runs over $b_1, c_1, b_2, c_2, b_3, c_3 \in \{0, 1\}$. In this project we showed that $(\rho, U^\dagger, d)$ is a quantum correlated equilibrium (allowing the players to make arbitrary quantum operations) with expected payoff 7/4 for each player—higher than the classical equilibrium payoff.

Notice that there is some arbitrariness in this construction of a quantum version of the Public Goods game, associated with the choice of the maps d_i. The choice above forces each player to contribute if either of his qubits is measured to be in the state $|1\rangle$. An alternative choice for the interpretation of computational basis vectors as classical strategies is:

$$d'_i : |bc\rangle \mapsto \begin{cases} 1 & \text{with probability } (b+c)/2; \\ 0 & \text{with probability } 1-(b+c)/2, \end{cases}$$

so that if both qubits are measured to be $|1\rangle$ or $|0\rangle$, the player contributes 1 or 0, respectively, while if one qubit is measured to be $|0\rangle$ and the other to be $|1\rangle$, then the player contributes 1 with probability 1/2.

In this case we showed that (ρ, V, d') is a quantum correlated equilibrium and the expected payoffs are 145/96 for each player, which is less than 7/4, but still greater than 1.

7.4 Other Adversarial Quantum Communication Protocols

Hogg, Harsha and Chen have a proposal for a quantum auction protocol [24], but it requires multiple rounds of (coherent) communication, which makes it less amenable to near-term experimental implementation than the Public Goods game with quantum communication. In addition, their protocol has not been checked for robustness against arbitrary cheating strategies, and in our judgement is not likely to be robust.

In this seedling project, therefore, we focussed on another adversarial communication task, Symmetrically Private Information Retrieval (SPIR), namely, the problem of querying a database of size N while keeping the query private from the database owner and revealing only the queried register of the database [25]. It is easy to see that query privacy can be achieved by delivering the whole database, while database privacy can be achieved by responding only to a single query. The communication complexity of classical protocols achieving both is $O(N)$ [25].

Hogg and Zhang have considered *quantum* protocols for SPIR [26]. Giovannetti, Lloyd and Maccone (GLM) recently proposed an *efficient* quantum SPIR protocol [27]. As an abstraction of the notion of a database, consider a set of registers $\{0, \ldots, N-1\}$ with contents described by a function $f : \{0, \ldots, N-1\} \to G$, where G is an abelian group (under addition) and $f(0) = 0$. Then the correct response to a query $x \in \{0, \ldots, N-1\}$ is $f(x)$; this is implemented quantum mechanically by the unitary operator defined by $U_f : |x\rangle|g\rangle \mapsto |x\rangle|g + f(x)\rangle$, where $|x\rangle$ is a computational basis vector in an N dimensional

Hilbert space and $|g\rangle$ is a computational basis vector in a $|G|$ dimensional Hilbert space. The intended GLM protocol is:

1. The querier prepares the state $|x\rangle|0\rangle$ and the state $\big(|x\rangle|0\rangle + |0\rangle|0\rangle\big)/\sqrt{2}$;
2. The querier then sends one of these two states, at random, to the database owner;
3. The database owner applies U_f to the state he receives and returns the result;
4. After receiving the response to his first query, the querier sends the remaining state to the database owner;
5. The database owner applies U_f to the state he receives and returns the result;
6. From the $|x\rangle|f(x)\rangle$ response the querier can determine $f(x)$ and then check that the other response is correct, *i.e.*, that the database owner has not observed the query.

Giovanetti, Lloyd and Maccone provide a privacy analysis of this protocol in [28].

The GLM protocol provides a family of increasingly complicated, but scalable (since the communication complexity is $O(\log N)$), possible quantum communication experiments. For this part of the seedling project we analyzed the complexity of implementing the simplest non-trivial instance of the GLM protocol, namely one with a 2 bit database, $N = 4$, of bits, so there are $2^3 = 8$ possible databases f.

In this case the querier must be able to produce a state $|x\rangle = |b_1 b_0\rangle$, where b_0 and b_1 are bits. This requires only single-qubit operations. The querier must also be able to produce the superposition state $\big(|x\rangle + |0\rangle\big)/\sqrt{2} = \big(|b_1 b_0\rangle + |00\rangle\big)/\sqrt{2}$, for $0 \neq x = 2b_1 + b_0$. This requires single-qubit operations, and one controlled-NOT operation when $x = 3$.

The database owner must be able to implement the three-qubit operation U_f. Of the 8 possible databases f in this case, some are represented by very simple U_f, *e.g.*, $f(x) = 0$ has $U_f = I_8$, the eight-dimensional identity matrix. The most complicated cases are exemplified by the database with $f(3) = 1$ and $f(0) = f(1) = f(2) = 0$, for which U_f is the controlled-controlled-NOT operation. This operation can be implemented using six controlled-NOT operations [29], or more efficiently using a scheme of Ralph, Resch and Gilchrist that only uses three two-particle operations, but does require that one of them be a qutrit, *i.e.*, a 3-level system [30]. If the third level is implemented by a third spatial mode/optical path, and a single-qutrit operation interchanging the first and third levels is available, then the three two-particle operations can all be implemented using exactly the same architecture as two-qubit controlled-NOT operations targeting the first two levels of the qutrit.

7.5 Security Benefits of Quantum Communication in Adversarial Scenarios

As the GLM quantum protocol for SPIR described in the previous subsection illustrates, there can be security benefits to using quantum communication in adversarial scenarios.

Furthermore, by definition, the quantum correlated equilibrium for the PUBLIC GOODS game is robust against unilateral deviations by the players. We also demonstrated that in the state ρ prepared by the referee, each shared pair of qubits is in the *very mixed* state

$(|00\rangle\langle 00| + |11\rangle\langle 11|)/2$, which is effectively classical, making it robust against decoherence-type errors.

8 Conclusion

8.1 Summary of Results

The main purpose of this seedling was to verify the feasibility of experimental quantum games. Although the proof-of-principle implementation of a quantum public goods game fulfilled this purpose, there were several other important experimental and theoretical successes which made that experiment possible.

Experimentally, each component of the quantum game represents an important advance over previous research. The LOQC-compatible source of entangled photons developed for this seedling is the first telecom-band source of degenerate entangled photons, and was measured to have a 96 ± 1% fidelity with a maximally entangled state. The process fidelity of the controlled-NOT gate was—for the first time—directly measured, and bounded to between 91% and 95%. The four-detector array used for game readout represents a considerable technological improvement over previous detection schemes.

Theoretical progress began with the formalization of the quantum public goods game and the classification of its equilibria. We additionally reclassificatied quantum games as adversarial quantum communications protocols (in contrast to cooperative quantum communications protocols, such as quantum key distribution). From within this broader class of adversarial protocols we performed a detailed analysis of the SYMMETRIC PRIVATE INFORMATION RETRIEVAL protocol, and concluded that it is an ideal candidate for near-term experimental implementation.

Finally, the quantum game itself was successfully demonstrated. Quantum game performance clearly exceeded classical game peformance (by a ratio which increases linearly with the number of players), and was within statistical errors of the theoretical predictions.

8.2 Milestones

8.2.1 Experimental Milestones

(Experimental efforts comprised roughly 5/6 of the total program).

1. Construct and characterize a degenerate, polarization entangled source of photon pairs in the 1550-nm telecommunications band.

   Complete: The entangled source had a fidelity of 96 ± 1% with a maximally entangled state and a HOM dip visibility of 97 ± 4%.

2. Connect this source of degenerate, polarization entangled photon pairs, a pair of unitary transformations (which are used to implement the players' strategies), an entangling gate, and a measurement / detection array. Verify the operation of this joint system.

Complete: The operation was verified for both classical and quantum game moves, resulting in average truth table fidelities of $82 \pm 4\%$ and $77 \pm 4\%$, respectively.

3. Use this system to verify in a proof-of-principle experiment that a quantum public goods game is feasible.

   Complete: The quantum game exceeding the classical performance by amount which linearly increased with number of players. Experimental data was within error of theoretical predictions. (See Figure 10).

8.2.2 Theoretical Milestones

(Theoretical efforts comprised roughly 1/6 of the total program).

1. Find and classify the equilibria for the quantum public goods game.

   Complete: We have classified the equilibria for both proposed versions of the quantum public goods game, with calculated payoffs of 7/4 and 145/96 respectively (see Section 7.3).

2. Investigate a development blueprint for a next-generation quantum protocol.

   Complete: Although we originally planned on developing a quantum auction protocol, more detailed analysis showed no significant advantage over classical analogues. We instead investigated the development blueprint for the SYMMETRIC PRIVATE INFORMATION RETRIEVAL protocol (see Section 7.4).

3. Investigate security arrangements necessary to keep player strategies secret from a referee, or, put more generally, investigate how quantum protocols can add security to competitive situations (as opposed to collaborative situations, as in quantum key distribution).

   Complete: We have investigated the security proof for the SPIR protocol (see Section 7.5).

4. Investigate possibility of performing quantum games over metro distances.

   Complete: We conclude that the best choice for near-term, metro-distance implementation of a quantum game is the SPIR protocol.

References

[1] Kay-Yut Chen, Tad Hogg, and Raymond Beausoleil. A quantum treatment of public goods economics. *Quant. Inf. Proc.*, 1(6):449–469, 2002.

[2] R. Stolen and J. Bjorkholm. Parametric amplification and frequency conversion in optical fibers. *Quantum Electronics, IEEE Journal of*, 18(7):1062–1072, Jul 1982.

[3] D.B. Mortimore. Fiber loop reflectors. *Lightwave Technology, Journal of*, 6(7):1217–1224, Jul 1988.

[4] J. Chen, K. F. Lee, and P. Kumar. Deterministic quantum splitter based on time-reversed Hong-Ou-Mandel interference. *Physical Review A*, 76(3):031804, September 2007.

[5] Xiaoying Li, Paul L. Voss, Jay E. Sharping, and Prem Kumar. Optical-fiber source of polarization-entangled photons in the 1550 nm telecom band. *Phys. Rev. Lett.*, 94(5):053601, Feb 2005.

[6] P. Kumar, M. Florentino, P. L. Voss, and J. E. Sharping, 'All-fiber photon-pair source for quantum communications', U.S. Patent No 6,897,434 (2005).

[7] Kim Fook Lee, Jun Chen, Chuang Liang, Xiaoying Li, Paul L. Voss, and Prem Kumar. Generation of high-purity telecom-band entangled photon pairs in dispersion-shifted fiber. *Opt. Lett.*, 31(12):1905–1907, 2006.

[8] J. B. Altepeter, E. R. Jeffrey, P. G. Kwiat, S. Tanzilli, N. Gisin, and A. Acín. Experimental Methods for Detecting Entanglement. *Physical Review Letters*, 95(3):033601–+, July 2005.

[9] Joseph B. Altepeter, Evan R. Jeffrey, and Paul G. Kwiat. *Advances in AMO Physics, 2006, Chapter 3: Photonic State Tomography.* Elsevier, Munich, Germany, 2006.

[10] We define general Bell fidelity F_G as the state fidelity between a given state, ρ, and the maximally entangled state $|\psi_{\alpha,\beta,\phi}\rangle = \frac{1}{\sqrt{2}}(|\alpha\rangle|\beta\rangle + e^{\imath\phi}|\alpha^{\perp}\rangle|\beta^{\perp}\rangle)$ to which it is closest: $F_G(\rho) \equiv \forall_{\alpha,\beta,\phi}\max[F(\rho, |\phi_{\alpha,\beta,\phi}\rangle\langle\psi_{\alpha,\beta,\phi}|)]$.

[11] Daniel F. V. James, Paul G. Kwiat, William J. Munro, and Andrew G. White. Measurement of qubits. *Phys. Rev. A*, 64:052312, 2001.

[12] L. Mandel and E. Wolf. *Optical coherence and quantum optics.* Cambridge University Press, 1995.

[13] C. Liang, K. F. Lee, M. Medic, P. Kumar, R. H. Hadfield, and S. W. Nam. Characterization of fiber-generated entangled photon pairs with superconducting single-photon detectors. *Optics Express*, 15:1322–1327, February 2007.

[14] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, UK, 2000.

[15] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409:46, January 2001.

[16] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn. Linear optical quantum computing with photonic qubits. *Reviews of Modern Physics*, 79:135–174, January 2007.

[17] H. F. Hofmann. Complementary Classical Fidelities as an Efficient Criterion for the Evaluation of Experimentally Realized Quantum Operations. *Physical Review Letters*, 94(16):160504, April 2005.

[18] J. Chen, J. B. Altepeter, M. Medic, K. F. Lee, B. Gokden, R. H. Hadfield, S. W. Nam, and P. Kumar. Demonstration of a Quantum Controlled-NOT Gate in the Telecommunications Band. *Physical Review Letters*, 100(13):133603, April 2008.

[19] J. Eisert, M. Wilkens, and M. Lewenstein. Quantum Games and Quantum Strategies. *Physical Review Letters*, 83:3077–3080, October 1999.

[20] L. Marinatto and T. Weber. A quantum approach to static games of complete information. *Physics Letters A*, 272:291–303, August 2000.

[21] D. A. Meyer. Quantum Communication in Games. In S. M. Barnett, E. Andersson, J. Jeffers, P. Öhberg, and O. Hirota, editors, *American Institute of Physics Conference Series*, volume 734 of *American Institute of Physics Conference Series*, pages 36–39, November 2004.

[22] Kay-Yut Chen, Tad Hogg, and Raymond Beausoleil. A quantum treatment of public goods economics. *Quantum Information Processing*, 1(6):449–469, 2002.

[23] Robert J. Aumann. Subjectivity and correlation in randomized strategies. *Journal of Mathematical Economics*, 1(1):67–96, March 1974.

[24] T. Hogg, P. Harsha, and K.-Y. Chen. Quantum Auctions. *ArXiv e-prints*, April 2007.

[25] Yael Gertner, Yuval Ishai, Eyal Kushilevitz, and Tal Malkin. Protecting data privacy in private information retrieval schemes. In *STOC '98: Proceedings of the thirtieth annual ACM symposium on Theory of computing*, pages 151–160, New York, NY, USA, 1998. ACM.

[26] T. Hogg and L. Zhang. Private Database Queries Using Quantum States with Limited Coherence Times. *ArXiv e-prints*, September 2007.

[27] V. Giovannetti, S. Lloyd, and L. Maccone. Quantum Private Queries. *Physical Review Letters*, 100(23):230502, June 2008.

[28] V. Giovannetti, S. Lloyd, and L. Maccone. Quantum Private Queries: security analysis. *ArXiv e-prints*, September 2008.

[29] A. Barenco, C. H. Bennett, R. Cleve, D. P. Divincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Physical Review A*, 52:3457–3467, November 1995.

[30] T. C. Ralph, K. J. Resch, and A. Gilchrist. Efficient Toffoli gates using qudits. *Physical Review A*, 75(2):022313, February 2007.